O aplicativo de visualização digital, ou DVA, fornece ao Exército uma solução de comutação de vídeo baseada em software e permite que os integrantes do posto de comando conectem com a rede local para compartilhar toda ou parte de sua tela com outros indivíduos ou com o sistema geral do posto de comando. (Foto simulada: cedida pelo Exército dos EUA)

Como Localizar o Inimigo no Campo de Batalha Inundado por Dados de 2035

Cap T. S. Allen, Exército dos EUA

Para localizar o inimigo atualmente, forças armadas apontam meios de coleta de informações — que podem identificar qualquer coisa, desde uma assinatura visual até uma radiofrequência específica — em direção à área onde creem que o inimigo se encontra, até localizá-lo. Esse modelo está

desatualizado porque o crescimento do ciberespaço, que se converteu em uma rede de controle global que interconecta dispositivos, criou um novo campo de batalha, "inundado por dados" e coberto por bilhões de dispositivos em rede, que compartilham informações constantemente e podem ser explorados para localizar o inimigo de forma mais eficiente.[1]

Até 2035, as forças armadas no campo de batalha inundado por dados passarão, normalmente, a localizar o inimigo por meio da exploração de dados no ciberespaço e no ambiente informacional mais amplo, em lugar de monitorar forças inimigas diretamente com seus próprios meios de coleta de informações.[2] Em termos mais claros, o inimigo vai transmitir onde está, ou terceiros vão transmitir onde ele está, tantas vezes quanto forças armadas apontarem uma câmera ou antena para ele a fim de localizá-lo. Forças armadas consultarão constantemente uma grande variedade de bancos de dados, tanto de informações do ciberespaço disponíveis publicamente quanto das adquiridas de modo sigiloso, para identificar indicadores da localização do inimigo. Em vez de efetuar uma varredura visual ou eletrônica para detectar o inimigo, as forças armadas mais eficientes o buscarão em algo como o Google, utilizando ferramentas de inteligência que exploram o ciberespaço.

No campo de batalha inundado por dados, a força armada mais preparada para explorar o ciberespaço a fim de localizar o inimigo terá uma vantagem significativa. O Exército dos Estados Unidos da América (EUA) precisa desfazer e reformular seu modelo de inteligência tática a fim de se preparar para vencer nessas condições.

Como localizar alvos no campo de batalha de 2035

A transformação da inteligência tática de modo a torná-la centrada no ciberespaço já está em curso.[3] Os inimigos dos EUA têm visado suas forças com base em postagens nas mídias sociais após lapsos de segurança operacional desde pelo menos 2007.[4] Por sua vez, as Forças Armadas dos EUA lançaram bombas contra terroristas que cometeram o erro de postar selfies revelando sua localização.[5] À medida que aumentarem o número de dispositivos conectados em rede e a frequência com que as pessoas os utilizam para transmitir informações intencionalmente ou não, a utilidade dos fluxos existentes de dados cibernéticos para identificar a localização de qualquer coisa, seja um consumidor ou uma viatura de combate blindada, também continuará a crescer.[6] Futuramente, é quase certo que o ciberespaço e o ambiente informacional mais amplo se tornarão a principal fonte de inteligência dos EUA, incluindo inteligência tática sobre a localização e disposição de forças inimigas. As forças estadunidenses continuarão a utilizar meios tradicionais de coleta de informações para identificar a localização de tropas inimigas e fixá-las, mas também se apoiarão cada vez mais em informações do ciberespaço para determinar, em primeiro lugar, para que direção devem apontar tais sensores. Afinal de contas, não há necessidade de patrulhar uma província inteira, buscando uma coluna de carros de combate inimigos, quando alguém tuita uma selfie que os mostra em segundo plano ou quando o movimento da coluna ao longo de uma rodovia provoca uma enorme alteração nos padrões de trânsito civil que possa ser facilmente identificada com base nos dados colhidos por aplicativos de navegação de celulares.

Até hoje, a transformação da inteligência tática pelo ciberespaço tem sido mais evidente na disciplina de inteligência de fontes abertas (*open-source intelligence*, OSINT). Desde o nascimento da "Social Web", também conhecida como "Web 2.0", no final da década de 1990, o conteúdo gerado por usuários nas mídias sociais tem sido central na cultura da internet. Além disso, os smartphones, que permitem que os usuários façam o upload de conteúdo de praticamente qualquer lugar e captem e divulguem imagens rapidamente, passaram a funcionar como bilhões de dispositivos de coleta de informações conectados em rede, que compartilham publicamente muitos de seus resultados nas mídias sociais. Isso tem

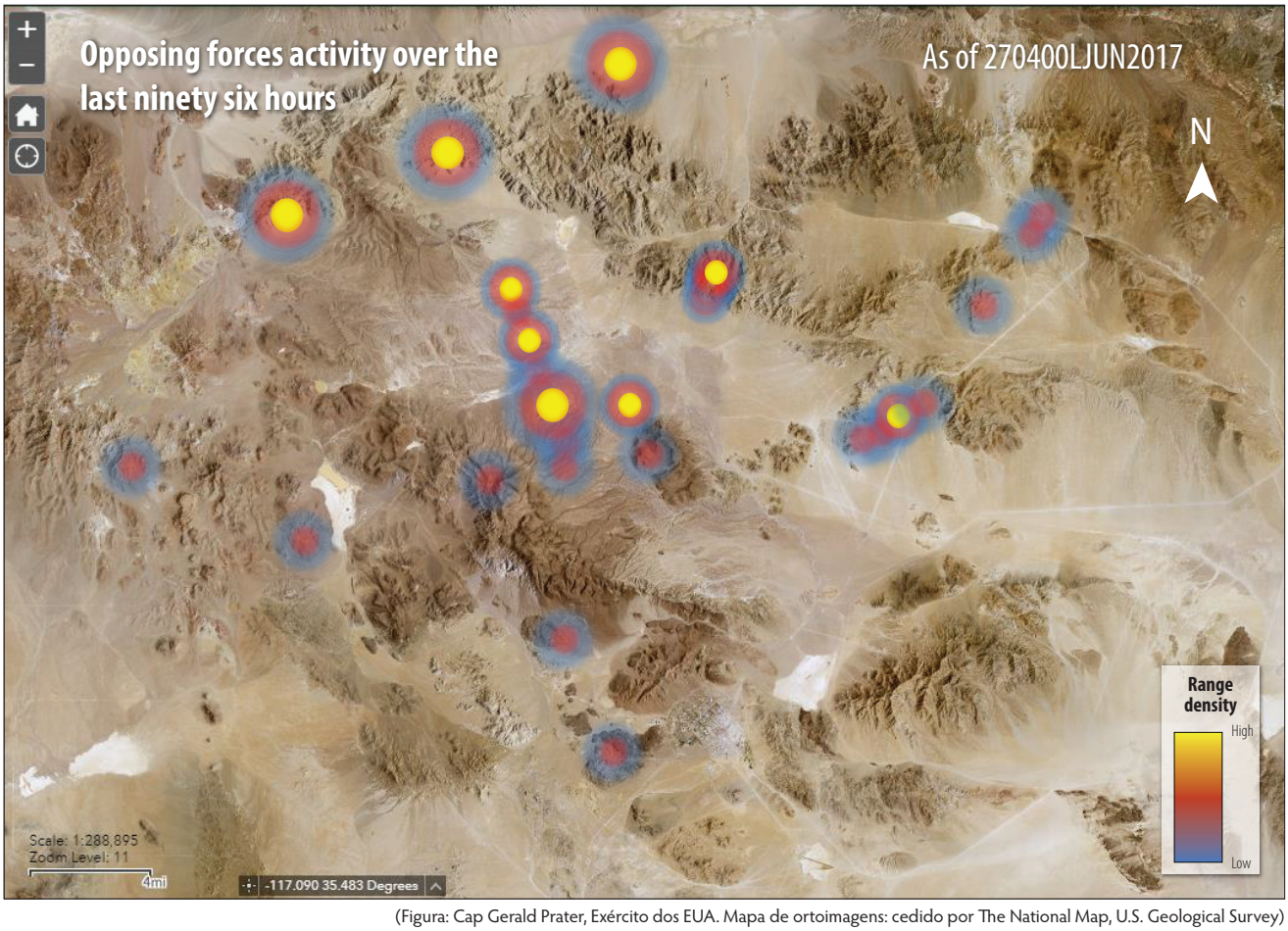
O Cap T. S. Allen, do Exército dos EUA, é oficial de inteligência militar e serve junto ao Asymmetric Warfare Group em Fort George G. Meade, Maryland. Serviu, anteriormente, no Afeganistão e na Coreia, sendo qualificado para planejar operações cibernéticas e de informação. O Cap Allen é bacharel em Ciência Política e História Militar pela Academia Militar dos EUA em West Point e mestre em Estudos de Guerra pelo King's College London.

Militares configuram o modo "estender" do ambiente computacional tático, que reúne vários pontos em um mapa digital para gerar uma imagem mais ampla, semelhante à disponível em postos de comando maiores. Essa tecnologia pode ajudar os militares a colaborar e aumenta a consciência situacional em uma formação por meio do compartilhamento de um cenário operativo comum quase em tempo real do "campo de batalha inundado por dados". (Foto: cedida pelo Exército dos EUA)

levado à proliferação de informações publicamente disponíveis com valor operacional e de inteligência.[7] Até mesmo organizações civis hoje têm a capacidade de conduzir avaliações de inteligência com um elevado grau de exatidão utilizando esses dados. Em um exemplo conhecido, a entidade Atlantic Council e o canal de internet Vice News conseguiram identificar, individualmente, soldados russos que combatiam secretamente na Ucrânia, com base em sua atividade nas mídias sociais em 2014.[8] Da mesma forma, o site de jornalismo investigativo Bellingcat tem conseguido fornecer, regularmente, avaliações de inteligência de alta qualidade, baseadas quase exclusivamente no que ele denomina "inteligência de fontes abertas" proveniente das mídias sociais. Conforme observa o analista civil de fontes abertas Cameron Colquhoun: "Entre os bilhões de postagens, uploads, compartilhamentos e curtidas, as pessoas revelam seus interesses repetidas vezes a observadores meticulosos".[9]

No entanto, com base em minha experiência como oficial de inteligência, a OSINT não se tornou a principal fonte de inteligência tática. Em primeiro lugar, ela depende muito de que os usuários, que não são controlados ou submetidos a um processo de validação, compartilhem livremente informações sobre eventos de interesse. Os usuários têm fortes razões para não monitorar forças militares, que são armadas e perigosas. Mesmo quando o fazem, raramente monitoram de modo persistente e, como a inteligência tática é rapidamente perecível, a OSINT só é útil em raros casos para localizar o inimigo no nível tático.

Entre hoje e 2035, o ciberespaço concluirá outra enorme transformação, como a vista anteriormente com smartphones e mídias sociais, e os efeitos dela na inteligência tática serão ainda mais significativos. A nova transformação é impulsionada pela ascensão da "Internet das Coisas" (*Internet of Things*, IoT, ou, ainda, IdC). O ciberespaço já efetuou uma transição



(Figura: Cap Gerald Prater, Exército dos EUA. Mapa de ortoimagens: cedido por The National Map, U.S. Geological Survey)

Mapa de calor da localização das forças oponentes no Centro Nacional de Treinamento em 2017

Dois tenentes inovadores produziram o mapa usando dados de localização de mídias sociais, o qual poderia ter sido produzido de qualquer lugar do mundo, sem exigir nenhum equipamento especial de inteligência.

de rede de comunicação global que conecta pessoas para uma rede de controle global que conecta dispositivos, como afirma Laura DeNardis em *The Internet in Everything: Freedom and Security in a World with No Off Switch* ("A Internet em Tudo: Liberdade e Segurança em um Mundo sem Botão de Desligar", em tradução livre).[10] Os dispositivos hoje são responsáveis por mais atividade no ciberespaço que as pessoas, e o ciberespaço é utilizado para controlar tudo, desde termostatos em residências particulares a sistemas de controles industriais em fábricas. Como a IoT é, em grande medida, automatizada, os usuários cujo comportamento incontrolável limitava a utilidade tática da OSINT proveniente da Web 2.0 agora são irrelevantes. "Se os seres humanos desaparecessem subitamente da Terra", afirma DeNardis, "o mundo digital continuaria a zumbir vibrantemente".[11] A doutrina cibernética do Exército dos EUA provavelmente mudará para refletir isso. Embora as atuais descrições doutrinárias do ciberespaço enfatizem que ele é "socialmente capacitador", o Exército já tem várias razões para também caracterizá-lo como "amplamente automatizado".[12]

A IoT oferece oportunidades interessantes de inteligência tática. Se as operações de inteligência e cibernéticas forem integradas de forma eficaz, a IoT poderá tornar-se uma inédita mina de ouro de informações, proporcionando aos agentes de coleta de inteligência acesso a inúmeros sensores para localizar o inimigo. Enquanto os EUA tentaram, durante

a Guerra do Vietnã, monitorar grandes áreas por meio do lançamento aéreo de milhares de sensores na selva, no futuro, objetivos semelhantes poderiam ser alcançados por meio da exploração de sensores civis já em uso.[13] Dispositivos como câmeras de segurança residencial têm informações com valor de inteligência se estiverem apontados para o local certo. Como eles se tornaram bastante comuns, é certo que alguns sensores de IoT estarão apontados para áreas de interesse durante pelo menos parte do tempo. Além disso, os dispositivos de IoT são notoriamente inseguros, conforme demonstrado regularmente por hackers.[14] No início de 2020, 98% do tráfego de IoT não estava encriptado, tornando-o extraordinariamente fácil de explorar.[15] As principais desvantagens de explorar sensores de IoT são que eles não podem ser tecnicamente controlados e são vulneráveis à dissimulação e à manipulação, mas essas deficiências serão compensadas pela enorme escala de dados disponíveis, que podem ser utilizados para acrescentar cada vez mais informações como base para avaliações.

À medida que a IoT evolui, uma significativa prática que vem se tornando comum é o fato de que a maioria dos veículos transmite dados sobre sua localização. Embora o Exército dos EUA não vá encontrar o inimigo dentro do país primordialmente, as práticas cibernéticas estadunidenses frequentemente proliferam por todo o mundo, sendo, assim, um importante indicador. Nos EUA, atualmente, todas as aeronaves já emitem sua localização por meio de um sistema denominado vigilância dependente automática por radiodifusão (*automatic dependent surveillance–broadcast*, ADS-B), e a maioria dos navios faz o mesmo por meio do sistema de identificação automática. O Departamento de Transporte dos EUA também defende o emprego de sistemas de comunicação de segurança veículo a veículo para a maioria dos automóveis particulares, que transmitiriam dados de localização.[16] Até 2035, sistemas como ADS-B, sistema de identificação automática e comunicação veículo a veículo irão quase certamente propagar-se por todo o mundo. Embora esses sistemas tenham sido projetados para proporcionar segurança e um mínimo de privacidade, na prática, como eles ainda compartilham dados de localização, eles possibilitarão que qualquer dispositivo automático devidamente equipado monitore facilmente todos os movimentos veiculares. Além disso, se o sistema ADS-B pode servir de indicação, é provável que sensores fixos que monitoram atividades de movimento e as compartilham automaticamente no ciberespaço se tornem comuns, para satisfazer a demanda do público por dados sobre o trânsito. Conforme constatado pelo Government Accountability Office (equivalente estadunidense ao tribunal de contas) em uma avaliação dos sistemas ADS-B realizada em 2018, eles representam graves riscos para a segurança operacional de forças militares, incluindo as nossas, porque poderiam exigir a transmissão da localização de atividades militares sigilosas.[17]

Existe também uma nova, mas contestada regra, com base na qual os seres humanos compartilham dados sobre sua localização para o ciberespaço por meio de seus telefones e outros dispositivos de IoT portáteis. O Departamento de Defesa recebeu um chocante alerta sobre isso em 2018, quando a Strava, uma empresa de dispositivos de monitoramento de

Um mapa de calor de 2018 mostra o movimento de militares com base em dados de localização colhidos do aplicativo de monitoramento de atividades físicas Strava na Base Aérea de Bagram, no Afeganistão (Captura de tela: cedida por Strava Labs)

atividades físicas, publicou um mapa de calor baseado nos usuários, que destacava rotas de corrida em bases militares em todo o mundo.[18] Recebeu outro em 2019, quando o *The New York Times* reportou que havia utilizado dados de localização de celulares para acompanhar os movimentos de um alto funcionário do Departamento de Defesa.[19] É provável que o compartilhamento de dados de localização continue porque, conforme observa Shoshanna Zuboff, as empresas lucram com sua exploração e a maioria dos usuários está disposta a fornecê-los. Embora muitas pessoas se incomodem com a ideia de estarem sendo rastreadas individualmente, elas geralmente têm poucas objeções contra o compartilhamento de dados rotulados como "agregados" ou "anônimos".[20] A pandemia da covid-19 gerou uma atenção bem maior do público para rastreadores de localização de telefones celulares.[21] Durante a pandemia, o Google utilizou seu banco de dados de localização de usuários de smartphones para fornecer relatórios detalhados aos funcionários de saúde pública sobre padrões de vida em todo o mundo, divulgando-os publicamente.[22] Em um caso de emprego mais pertinente, uma empresa de análise geoespacial da iniciativa privada relatou que fábricas de armamento russas estavam desacelerando a produção com base na utilização de dados semelhantes, para verificar quantos operários estavam indo trabalhar durante a pandemia.[23] Curiosamente, apenas cinco dias depois, o governo russo proibiu os militares de portar smartphones que monitoram a localização do usuário.[24]

Até 2035, então, passaremos a viver em um mundo onde a maioria dos movimentos gera uma assinatura no ciberespaço. Será fácil rastrear o movimento de veículos, e, no mínimo, as tendências gerais no movimento de indivíduos serão visíveis. É provável que ninguém vá instalar sistemas de rastreamento em veículos militares, mas isso não reduzirá o valor de inteligência dessa enorme fonte de dados. As forças militares manobrarão através de um campo de batalha inundado por dados, onde todas as ações "ocultas" que elas tomem produzirão uma reação fácil de monitorar. Mesmo que não emitam nada, elas serão indiretamente visíveis no ciberespaço quando alterarem os padrões de vida normais, quando provocarem engarrafamentos em rodovias, quando as pessoas publicarem informações sobre suas atividades nas mídias sociais e quando entrarem no campo de visão de dispositivos de IoT que possam ser explorados, como câmeras de segurança. Em muitos casos, os analistas serão capazes de localizar o inimigo por meio da identificação de mudanças nos padrões de vida normais, as quais mostrem uma *inatividade atípica* em uma determinada área. Chamo isso de "inteligência negativa", à semelhança do vazio significativo representado pelo "espaço negativo" nas mídias visuais. Ainda que as organizações militares possam não produzir, necessariamente, fogos letais contra alvos identificados apenas no ciberespaço, ele fornecerá a base de informações na qual as forças de inteligência localizarão o inimigo. Os meios tradicionais de coleta de informações continuarão a desempenhar um papel importante, mas se concentração em fixar forças inimigas encontradas no ciberespaço. A força que estiver mais preparada para acessar a grande variedade de informações com valor de inteligência no ciberespaço terá uma vantagem decisiva sobre outra força que se limite a um número menor de meios de coleta tecnicamente controlados, que só poderão colher uma quantidade de dados exponencialmente menor.

Este não é o campo de batalha que se busca

O campo de batalha inundado por dados de 2035 apresenta não só excelentes oportunidades de inteligência, mas também desafios tremendos para o Exército dos EUA. Para obter uma vantagem decisiva, o Exército deve efetuar mudanças fundamentais em seu modelo de inteligência tática, até mesmo além das delineadas em *The U.S. Army in Multi-Domain Operations 2028* ("O Exército dos EUA em Operações em Múltiplos Domínios 2028", em tradução livre), que descreve sua visão futura, mas não menciona IoT.[25] Essas mudanças são imprescindíveis, pois, caso não sejam implementadas, o Exército poderá ver-se diante de uma sobrecarga crônica de informações, tornando-se incapaz de executar o comando de missão e tendo de combater em futuras guerras sem muitas de suas vantagens históricas.

Em primeiro lugar, o Exército deve preparar-se para explorar informações do ciberespaço em núcleos de inteligência centralizados e altamente automatizados, voltados a apoiar o processo decisório tático, que identificarão, processarão, explorarão e disseminarão

informações com valor tático para as formações táticas como base para a ação. Historicamente, fazia sentido para o Exército deixar que os comandantes localizassem muitos de seus próprios alvos, porque eles podiam fazer isso com meios de coleta de informações de acesso próximo, em suas formações. Isso vai mudar com o campo de batalha inundado por dados, porque os dispositivos de IoT, em sua maioria, foram projetados para serem conectados em rede e compartilharem informações mundialmente, fazendo com que a questão de acesso próximo seja menos importante. Os dispositivos de IoT compartilham dados por meio de um ciberespaço que ficará cada vez mais "centralizado", com empresas enormes como a Tencent, na China, e a Yandex, na Rússia, controlando uma parcela sem precedentes de todos os dados.[26]

Ainda que a centralização da internet vá exigir a centralização da coleta de inteligência, o processo decisório do Exército deve permanecer amplamente distribuído, para manter a flexibilidade tática. Assim, os novos centros de inteligência terão de melhorar sua capacidade para disseminar o que sabem até o nível tático, predominantemente por meio de brigadas de inteligência militar existentes nos teatros de operações, agregadas a exércitos de campanha, para reforçarem sensores de acesso próximo.[27] Devido à enorme quantidade de dados a serem processados, a inteligência artificial e o aprendizado de máquina passarão a ser fundamentais para o processamento e exploração. Os gestores de coleta de inteligência no campo de batalha inundado por dados de 2035 modificarão algoritmos para atender às necessidades de informação. Caso contrário, é quase certo que eles enfrentem uma sobrecarga de informações — e falhas de inteligência.[28] O escalonamento das capacidades de inteligência e o aproveitamento de economias de escala em escalões mais elevados ajudarão a evitar a geração de uma sobrecarga de informações em escalões mais baixos.

Em segundo lugar, para explorar adequadamente o campo de batalha inundado por dados, o Exército deve romper barreiras entre as áreas de cibernética e de inteligência. As capacidades sofisticadas utilizadas atualmente para a inteligência, vigilância e reconhecimento no ciberespaço terão de ser adaptadas

Integrante da equipe de atividades cibernéticas e eletromagnéticas expedicionárias do 781º Batalhão de Inteligência Militar conduz operações cibernéticas em 9 de maio de 2017, no Centro Nacional de Treinamento, em Fort Irwin, Califórnia. Mais recentemente, o 915º Batalhão de Apoio ao Combate Cibernético, ativado em 1º de janeiro de 2019, representa a primeira capacidade expedicionária orgânica em escala para atender aos requisitos atuais e previstos do Exército dos EUA em relação a atividades cibernéticas e eletromagnéticas expedicionárias no nível tático. (Foto: Bill Roche, U.S. Army Cyber Command)

Integrantes do 6º Regimento de Operações Especiais usam um tablet para fazer o upload de coordenadas em 17 de dezembro de 2019 durante um exercício que demonstrou as capacidades do sistema avançado de gestão de combate (*advanced battle management system*, ABMS) em Duke Field, Flórida. Durante a primeira demonstração do ABMS, operadores da Força Aérea, do Exército, da Marinha e da indústria testaram várias ferramentas e tecnologias de compartilhamento de dados em tempo real em um cenário de defesa nacional concebido pelo U.S. Northern Command e implementado pela liderança da Força Aérea. (Foto: 2º Sgt Joshua J. Garcia, Força Aérea dos EUA)

para atender às necessidades de inteligência dos comandantes de manobra.[29] Em vez de simplesmente obter consciência situacional *do* ciberespaço, conforme estipula a doutrina atual, as forças cibernéticas terão de capacitar as forças de inteligência obtendo-a em relação a *todos os domínios por meio do ciberespaço*.[30] Isso exigirá que as forças de inteligência e as forças cibernéticas compartilhem informações de modo ininterrupto em apoio aos comandantes táticos, como parte da "convergência", ou seja, o objetivo do Exército de proporcionar a "integração rápida e contínua de todos os domínios ao longo do tempo, espaço e capacidades para superar o inimigo".[31]

Em terceiro lugar, o Exército precisa se preparar para o fato de suas próprias ações de nível tático serem visíveis no ciberespaço. Cada nova oportunidade de inteligência também é uma potencial ameaça à segurança operacional. O modelo de segurança de operações do Exército corre o risco de ficar desatualizado. Ele permanece centrado no controle de emissões, mas, até 2035, terá de controlar ou obscurecer as emissões dos dispositivos civis que monitorarão constantemente as forças do Exército no campo de batalha inundado por dados. Como é impossível controlar todos esses dispositivos, o obscurecimento e a dissimulação se tornarão mais importantes, até mesmo nos escalões táticos.[32] Os planejadores de segurança de operações do Exército também devem, cada vez mais, pensar "dois passos à frente" e preparar-se para combater e vencer, mesmo depois que suas atividades sejam divulgadas para o mundo todo. O Exército precisará, mais do que nunca, proporcionar capacidades avançadas de obscurecimento e dissimulação aos escalões inferiores, bem abaixo do nível de corpo de exército, atualmente o escalão mais baixo em que se prevê o emprego de capacidades de dissimulação

militar.[33] No campo de batalha inundado por dados, até as frações táticas precisarão do equivalente cibernético às máquinas de fumaça.

Em quarto lugar, o Exército deve tomar medidas deliberadas para preservar o comando de missão quando a tecnologia possibilitar o microgerenciamento. Conforme escreveu Marshall McLuhan em 1964: "No longo prazo, o conteúdo de um veículo é menos importante que o próprio veículo para influenciar a forma como pensamos e agimos".[34] Uma tecnologia avançada de comando e controle quase sempre prejudica o comando de missão, por facilitar o microgerenciamento. Quando o telégrafo foi usado pela primeira vez em operações militares na Guerra da Crimeia em 1855, o comandante francês constatou imediatamente que "a extremidade paralisante de um fio elétrico" havia feito com que fosse mais fácil para seus superiores em Paris dar ordens sem ter informações adequadas e mais difícil para ele responder a situações no terreno conforme se desenrolavam.[35] No futuro, quando um comandante de batalhão em um centro de operações tiver mais informações sobre a localização de uma força inimiga que um comandante de pelotão em contato com essa mesma força, ele se sentirá tentado a microgerenciar o comandante subordinado. No entanto, a flexibilidade do comando de missão continua a conferir uma vantagem decisiva às forças estadunidenses.[36] Assim, devemos tomar medidas cuidadosas para manter o comando de missão centrado no ser humano dentro de nossas forças, conforme a tecnologia avançar.

Em quinto lugar, o Exército precisa ser sensível às preocupações civis-militares-técnicas que surgirão no campo de batalha inundado por dados. Os "dados" são quase todos de propriedade exclusiva de empresas e controlados pela indústria privada. Embora as empresas privadas com acesso a eles participem de um mercado crescente de dados sobre as atividades de cidadãos privados em todo o mundo, os agentes comerciais de dados podem hesitar em compartilhar informações com forças armadas que as utilizarão para fins militares ou de inteligência. Os relacionamentos com esses agentes serão mais importantes do que nunca (e provavelmente mais tensos). Considerando os direitos de privacidade e outras preocupações legítimas quanto à proteção de dados, a exploração de dados sobre algum alvo estrangeiro que sejam de propriedade de empresas localizadas nos EUA ou nações aliadas continuará a ser uma questão problemática. Além disso, a exploração de dispositivos civis levantará, provavelmente, novas questões relacionadas ao direito dos conflitos armados.

Por fim, o Exército deve reconhecer que existe a real possibilidade de que seus adversários tenham uma vantagem no combate de inteligência tática ciberespacial. Muitas das vantagens em material conferidas pelos antigos meios sofisticados de coleta de informações do Exército serão menos importantes no campo de batalha inundado por dados, o que exigirá que a Força desenvolva novas vantagens, não relacionadas a materiais. Só porque os EUA têm liderado a revolução da informação não significa que o Exército esteja na melhor posição para dominar futuros campos de batalha.[37]

Muitos dos adversários dos EUA estão em condições de ultrapassar o país no campo da inovação. Conforme demonstra David Kilcullen em seu livro *The Dragons and the Snakes: How the Rest Learned to Fight the West* ("Os Dragões e as Serpentes: Como o Resto Aprendeu a Combater o Ocidente", em tradução livre), de 2020, os adversários dos EUA já os ultrapassaram por meio, em parte, da exploração de sistemas que o país construiu, originalmente, e, mais tarde, disponibilizou para o uso civil, como a internet e o GPS.[38] Como muitas atividades cibernéticas têm requisitos relativamente baixos em termos de recursos e, sobretudo, requerem adaptação a um ambiente cibernético em constante mudança, os atores não estatais ágeis e sem restrições têm vantagem sobre grandes burocracias estatais como o Exército.[39] Há sinais promissores de que o Exército também pode inovar, como os exemplos de soldados que descobriram como localizar forças inimigas por meio da exploração de aplicativos sociais como o Tinder e o Snapchat, que revelam dados de localização.[40] Embora os inovadores de escalões subordinados não possam estabelecer as soluções centralizadas e em escala de que o Exército precisa, a Força deve se empenhar mais em apoiar os hackers inovadores em suas fileiras.[41]

Conclusão

Os dados que cobrirão o campo de batalha de 2035 e que mudarão, fundamentalmente, a inteligência tática já estão se acumulando lentamente em bancos de dados em todo o mundo. Em campos de batalha futuros, os meios tradicionais de coleta de informações continuarão a desempenhar um papel crucial para possibilitar

que forças armadas fixem forças inimigas, mas, devido à proliferação de dispositivos em rede que transmitem automaticamente quantidades descomunais de dados na IoT, a fase *localizar* do processo de busca de alvos será centrada no ciberespaço. Para manter suas vantagens em campos de batalha futuros, o Exército deve aumentar sua capacidade para localizar o inimigo no ciberespaço em apoio à inteligência tática, começando agora.

Referências

1. Para uma discussão sobre o "fire-swept battlefield" ("campo de batalha varrido por fogos"), veja Stephen Biddle, *Military Power: Explaining Victory and Defeat in Modern Battle* (Princeton, NJ: Princeton University Press, 2004), p. 30. O termo "data-swept battlefield" (traduzido, neste artigo, por "campo de batalha inundado por dados") é do autor e original deste artigo. Trata-se de uma referência ao "campo de batalha varrido por fogos", que caracteriza o combate terrestre contemporâneo.

2. *DOD Dictionary of Military and Associated Terms* (Washington, DC: Department of Defense, as of June 2020), p. 55 e p.104, acesso em 15 set. 2020, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf?ver=2020-06-18-073638-727. "Ciberespaço" é definido como "domínio global dentro do ambiente informacional que consiste nas redes interdependentes de infraestruturas de tecnologia da informação e dados residentes, incluindo a internet, as redes de telecomunicações, os sistemas computacionais e os processadores e controladores embutidos". O "ambiente informacional" é definido como "o total agregado de indivíduos, organizações e sistemas que coletam, processam, disseminam ou agem com base em informações".

3. T. S. Allen and Robert A. Heber Jr., "Where Posting Selfies on Facebook Can Get You Killed", *Wall Street Journal* (site), 26 July 2018, acesso em 15 set. 2020, https://www.wsj.com/articles/where-posting-selfies-on-facebook-can-get-you-killed-1532642302.

4. "Insurgents Used Cell Phone Geotags to Destroy AH-64s in Iraq", Military.com, 15 March 2012, acesso em 15 set. 2020, https://www.military.com/defensetech/2012/03/15/insurgents-used-cell-phone-geotags-to-destroy-ah-64s-in-iraq.

5. Walbert Castillo, "Air Force Intel Uses ISIS 'Moron' Post to Track Fighters", CNN, 5 June 2015, acesso em 15 set. 2020, https://www.cnn.com/2015/06/05/politics/air-force-isis-moron-twitter/index.html?mod=article_inline.

6. Stuart A. Thompson and Charlie Warzel, "Twelve Million Phones, One Dataset, Zero Privacy", *New York Times* (site), 19 December 2019, acesso em 15 set. 2020, https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html.

7. Heather J. Williams and Ilana Blum, "Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise" (Santa Monica, CA: RAND Corporation, 2018), acesso em 15 set. 2020, https://www.rand.org/pubs/research_reports/RR1964.html.

8. "Selfie Soldiers: Russia Checks in to Ukraine", VICE News, 16 June 2015, acesso em 15 set. 2020, https://www.vice.com/en_us/article/bjk9na/selfie-soldiers-russia-checks-in-to-ukraine.

9. Cameron Colquhoun, "A Brief History of Open Source Intelligence", Bellingcat, 14 July 2016, acesso em 15 set. 2020, https://www.bellingcat.com/resources/articles/2016/07/14/a-brief-history-of-open-source-intelligence/.

10. Laura DeNardis, *The Internet in Everything: Freedom and Security in a World with No Off Switch* (New Haven, CT: Yale University Press, 2020).

11. Ibid., p. 3.

12. Field Manual (FM) 3-12, *Cyberspace and Electronic Warfare Operations* (Washington, DC: U.S. Government Publishing Office [GPO], 11 April 2017), para. 1-64, acesso em 15 set. 2020, https://armypubs.army.mil/ProductMaps/PubForm/Details.aspx?PUB_ID=1002097.

13. Matt Novak, "How the Vietnam War Brought High-Tech Border Surveillance to America", Gizmodo, 24 September 2015, acesso em 15 set. 2020, https://paleofuture.gizmodo.com/how-the-vietnam-war-brought-high-tech-border-surveillan-1694647526.

14. Joseph Cox and Samantha Cole, "How Hackers Are Breaking into Ring Cameras", VICE News, 11 December 2019, acesso em 15 set. 2020, https://www.vice.com/en_us/article/3a88k5/how-hackers-are-breaking-into-ring-cameras.

15. Unit 42, "2020 Unit 42 IoT Threat Report", Palo Alto Networks, 10 March 2020, acesso em 15 set. 2020, https://unit42.paloaltonetworks.com/iot-threat-report-2020/.

16. T. S. Allen, "Open-Source Intelligence: A Double-Edged Sword", *Proceedings* 144, no. 8 (August 2018), acesso em 15 set. 2020, https://www.usni.org/magazines/proceedings/2018/august/open-source-intelligence-double-edged-sword.

17. U.S. Government Accountability Office (GAO), *Homeland Defense: Urgent Need for DOD and FAA to Address Risks and Improve Planning for Technology That Tracks Military Aircraft* (Washington, DC: U.S. GAO, January 2018), acesso em 15 set. 2020, https://www.gao.gov/assets/690/689478.pdf.

18. Patrick Tucker, "Strava's Just the Start: The US Military's Losing War Against Data Leakage", Defense One, 31 January 2018, acesso em 15 set. 2020, https://www.defenseone.com/technology/2018/01/stravas-just-start-us-militarys-losing-war-against-data-leakage/145632/.

19. Thompson and Warzel, "Twelve Million Phones, One Dataset, Zero Privacy".

20. Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (New York: Hachette Book Group, 2019), p. 242-45.

21. Sara Morrison, "The Hidden Trackers in Your Phone, Explained", Vox, 8 July 2020, acesso em 15 set. 2020, https://www.vox.com/recode/2020/7/8/21311533/sdks-tracking-data-location.

22. "COVID-19 Community Mobility Reports", Google, última atualização em 13 set. 2020, acesso em 15 set. 2020, https://www.google.com/covid19/mobility/.

23. Patrick Tucker, "Russian Arms Production Slowed by Coronavirus, Analysts Find", Defense One, 1 May 2020, acesso em 15 set. 2020, https://www.defenseone.com/technology/2020/05/russian-arms-production-slowed-coronavirus-analysts-find/165071/.

24. "Putin Bans Armed Forces Members from Carrying Electronic Devices, Gadgets", Radio Free Europe/Radio Liberty, 7 May 2020, acesso em 15 set. 2020, https://www.rferl.org/a/putin-bans-armed-forces-members-from-carrying-electronic-devices-gadgets/30598888.html.

25. U.S. Army Training and Doctrine Command (TRADOC) Pamphlet (TP) 525-3-1, *The U.S. Army in Multi-Domain Operations 2028* (Fort Eustis, VA: TRADOC, 6 December 2018), acesso em 15 set. 2020, https://www.tradoc.army.mil/Portals/14/Documents/MDO/TP525-3-1_30Nov2018.pdf.

26. Prem Tummalacherla, "The Top 3 Issues of the Centralized Internet", Medium, 14 June 2019, acesso em 15 set. 2020, https://medium.com/@IamPremt/the-top-3-issues-of-the-centralized-internet-1db59d5e495e.

27. TP 525-3-1, *The U.S. Army in Multi-Domain Operations 2028*, p. 22.

28. Tom Lamont, "Can We Escape from Information Overload?", *The Economist* (site), 29 April 2020, acesso em 15 set. 2020, https://www.economist.com/1843/2020/04/29/can-we-escape-from-information-overload.

29. FM 3-12, *Cyberspace and Electronic Warfare Operations*, para. 1-41.

30. Ibid., para. 1-71.

31. TP 525-3-1, *The U.S. Army in Multi-Domain Operations 2028*, p. iii.

32. Edward Geist and Marjory Blumenthal, "Military Deception: Ai's Killer App?", War on the Rocks, 23 October 2019, acesso em 15 set. 2020, https://warontherocks.com/2019/10/military-deception-ais-killer-app/.

33. TP 525-3-1, *The U.S. Army in Multi-Domain Operations 2028*, p. 22.

34. Marshall McLuhan, apud Nicholas Carr, *The Shallows: What the Internet Is Doing to Our Brains* (New York: W. W. Norton, 2010), p. 3.

35. Gordon Wright, "Soldiers and Statesmen in 19th Century France", in *Soldiers and Statesmen: The Proceedings of the 4th Military History Symposium*, ed. Monte D. Wright and Lawrence J. Paszek (Washington, DC: Office of Air Force History, Headquarters USAF; and United States Air Force Academy, 1973), p. 28.

36. B. A. Friedman and Olivia A. Garard, "Technology-Enabled Mission Command", War on the Rocks, 9 April 2020, acesso em 15 set. 2020, https://warontherocks.com/2020/04/technology-enabled-mission-command-keeping-up-with-the-john-paul-joneses/.

37. Kenneth Pollack, "Society, Technology, and Future Warfare", American Enterprise Institute, 6 November 2019, acesso em 15 set. 2020, https://www.aei.org/research-products/report/society-technology-and-future-warfare/.

38. David Kilcullen, *The Dragons and the Snakes: How the Rest Learned to Fight the West* (New York: Oxford University Press, 2020), p. 38-65.

39. Stephen Rodriguez, "The Fox in the Henhouse: How Bureaucratic Processes Handicap US Military Supremacy and What to Do about It", Atlantic Council, 26 February 2020, acesso em 15 set. 2020, https://www.atlanticcouncil.org/blogs/new-atlanticist/the-fox-in-the-henhouse-how-bureaucratic-processes-handicap-us-military-supremacy-and-what-to-do-about-it/.

40. Curt Taylor, "It's Time for Cavalry to Get Serious about Cyber Reconnaissance", eArmor, Fall 2018, acesso em 15 set. 2020, https://www.benning.army.mil/Armor/eArmor/content/issues/2018/Fall/4Taylor18.pdf; Gina Harkins, "A Lance Corporal's Phone Selfie Got His Marine Unit 'Killed' at 29 Palms", Military News, 7 January 2020, acesso em 15 set. 2020, https://www.military.com/daily-news/2020/01/07/lance-corporals-phone-selfie-got-his-marine-unit-killed-29-palms.html.

41. James Long, "Shoot, Move, Communicate, and Innovate: Harnessing Innovative Capacity in the Ranks", Modern War Institute at West Point, 16 March 2020, acesso em 15 set. 2020, https://mwi.usma.edu/shoot-move-communicate-innovate-harnessing-innovative-capacity-ranks/.